networkMaryland

Customer Information Package

December 2002

Table of Contents

1- Introduction **1**

1.1. Purpose *1*

1.2. Roadmap *1*

1.3. Document Organization *1*

1.4. Acronyms *2*

1.5. Point of Contacts *2*

2- networkMaryland Benefits **3**

3 - networkMaryland Overview **4**

3.1 InterLATA Transport Services *4*

3.2 Internet Services *5*

3.3 Circuit Sizes *5*

4 - networkMaryland Connections **7**

4.1 Physical Connections *7*

4.2 Routing and Addressing Guidelines *8*

5 - networkMaryland Demarcation **10**

5.1 Local Loop Circuits *10*

5.2 Direct Private Fiber *11*

5.3 Twisted Pair Copper (CAT 5) for MAN Collocation *11*

6 - networkMaryland Service Levels **13**

7 - networkMaryland Acceptable Use Policy (10/2/02) **17**

8 - Customer Responsibilities **18**

9 - State of Maryland Data Security Policy (8/16/99) **19**

10 - Next Steps **30**

List of Figures

Figure 1. Roadmap – You Are Here 1
Figure 2. networkMaryland Design Overview 4
Figure 3. Maryland LATA Map 5
Figure 4. networkMaryland Connectivity Diagram 7
Figure 5. networkMaryland Demarcation Diagram 10
Figure 6. Roadmap – Get Pricing 30

List of Tables

Table 1. networkMaryland Team Point of Contacts 2

List of Version Changes

Date	Version	Changes
10/29/02	Final Draft *	▪ N/A
10/30/02	v1 *	▪ Added Figure 5, Demarcation Diagram. ▪ Added List of Version Changes. ▪ Renumbered Section 1.3. ▪ Corrected section references throughout the document. ▪ Deleted reference to a non-existent table in section 4.1.2.
11/18/02	v2 *	▪ Added footnote *. ▪ Reworded Section 1.1, Purpose. ▪ Added URL to the Roadmap in Section 1.2 and 10. ▪ Added NOC Acronym/Definition in Section 1.4 and 6. ▪ Reworded Section 2, paragraph 1 and 2. ▪ Clarified circuit ordering responsibilities in Section 4.1.1. ▪ Reworded Section 8, Customer Network Management.
12/16/02	v3 *	▪ Updated Figure 2, networkMaryland Design Overview.
12/30/02	v4 *	▪ Updated project contact information

* NOTE: The Department of Budget and Management attorney is in process of reviewing the Customer Information Package.

1- Introduction

1.1. Purpose

The purpose of this document is to provide value added and decision making information to potential customers about networkMaryland.

1.2. Roadmap

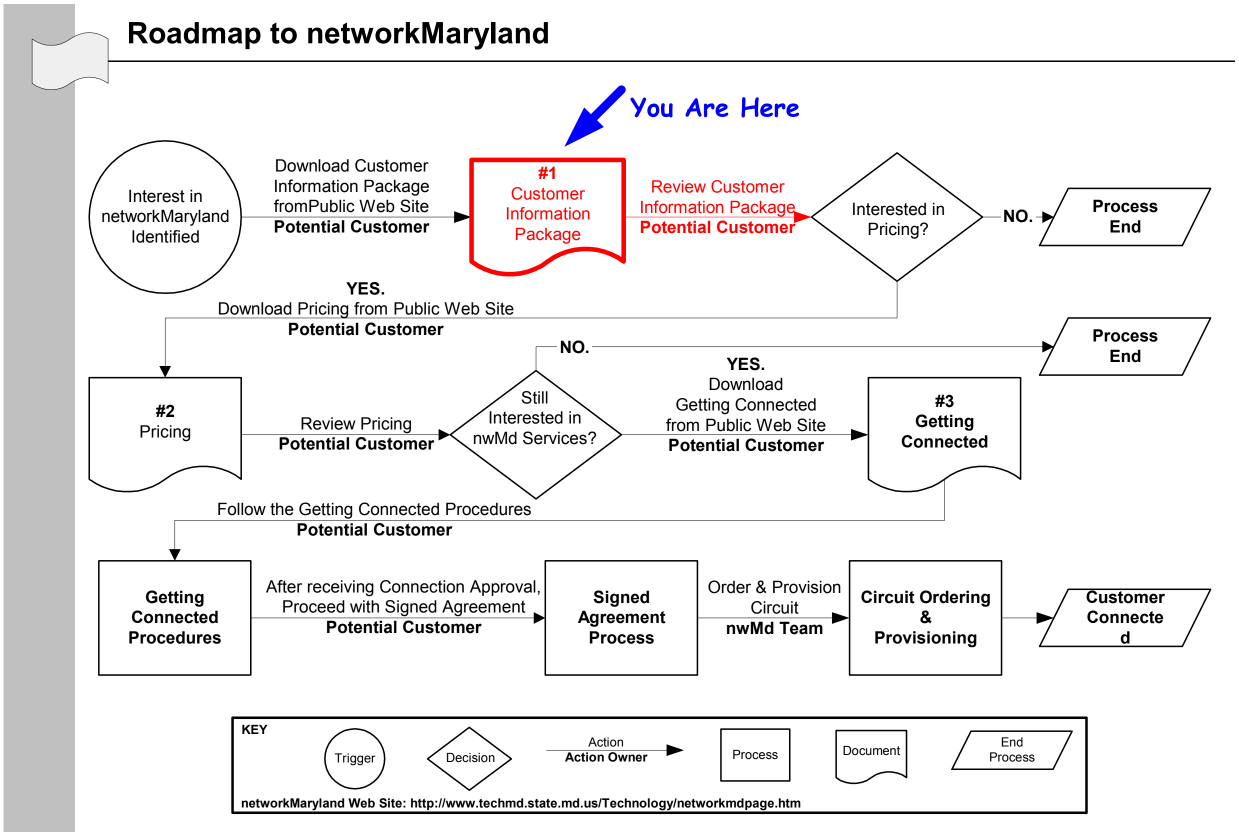
Roadmap to networkMaryland
You Are Here
Interest in networkMaryland Identified
Download Customer Information Package fromPublic Web Site
Potential Customer
#1 Customer Information Package
Review Customer Information Package
Potential Customer
Interested in Pricing?
NO.
Process End
YES.
Download Pricing from Public Web Site
Potential Customer
#2 Pricing
Review Pricing
Potential Customer
Still Interested in nwMd Services?
NO.
Process End
YES.
Download Getting Connected from Public Web Site
Potential Customer
#3 Getting Connected
Follow the Getting Connected Procedures
Potential Customer
Getting Connected Procedures
After receiving Connection Approval, Proceed with Signed Agreement
Potential Customer
Signed Agreement Process
Order & Provision Circuit
nwMd Team
Circuit Ordering & Provisioning
Customer Connecte d
KEY
Trigger
Decision
Action
Action Owner
Process
Document
End Process
networkMaryland Web Site: http://www.techmd.state.md.us/Technology/networkmdpage.htm

Figure 1. Roadmap – You Are Here

1.3. Document Organization

- Section 2 describes customer benefits of networkMaryland
- Section 3 contains an overview of networkMaryland
- Section 4 summarizes customer connections to networkMaryland
- Section 5 describes networkMaryland demarcations
- Section 6 details networkMaryland’s service levels
- Section 7 contains networkMaryland’s Acceptable Use Policy
- Section 8 outlines the customer’s responsibilities
- Section 9 contains the State of Maryland Data Security Policy
- Section 10 illustrates the next steps for connecting to networkMaryland

1.4. Acronyms

ATM: Asynchronous Transfer Mode
AUP: Acceptable Use Policy
CBR: Constant Bit Rate (ATM service class)
DS3: Digital Signal Level 3 (45 Mbps) utilizes a BNC Coaxial interface
InterLATA: Any network circuit that crosses from one defined geographic area into another.
ISP: Internet Service Provider
LAN: Local Area Network
LATA: Local Access Transport Area
LEC: Local Exchange Carrier
Local Loop: Physical network infrastructure that extends from the POP to customer premise
MAN: Metropolitan Area Network
nwMd Team: Members of the DBM's networkMaryland Team
NOC: Network Operating Center
PCR: Peak Cell Rate
PMO: Program Management Office
POP: Point of Presence (Network Access Point)
PVC: Permanent Virtual Circuit
PVP: Permanent Virtual Path
SCR: Sustained Cell Rate
UNI: User-Network Interface
VLAN: Virtual Local Area Network
VBR: Variable Bit Rate (ATM service class)
VCI: Virtual Channel Identifier
VPI: Virtual Path Identifier

1.5. Point of Contacts

Table 1. networkMaryland Team Point of Contacts

Name	Function	Phone #'s	Location
Margo Burnette	Project Director	410.260.7834	Annapolis
Mary Ann Slack	Project Manager	410.260.6126	Annapolis
Joe Scher	Project Controller	410.260.7284	Annapolis
Tim Kwong	Project Engineer	410.260.7423	Annapolis
Jason Ross	Project Engineer	410.260.7279	Annapolis
Email List: nwMd@dbm.state.md.us			

2- networkMaryland Benefits

The Department of Budget and Management created networkMaryland to support the networking needs of the State of Maryland. With the focus on supporting the advancement of higher education, health care and government services, networkMaryland strives to provide a high level of service. Whether the agency's needs are InterLATA networking, Internet Services or access to the State Intranet, networkMaryland can provide the connection desired. Utilizing this network will provide many benefits for the future.

networkMaryland benefits the State of Maryland by providing current and new services at higher data rates and lower prices. networkMaryland provides speeds from 1.5 Mbps - OC-48 (2.5 Gbps) to their customers depending on the solution. The services are available in 1 Mbps increments through the use of ATM technology providing a greater level of flexibility. This flexibility allows an agency to configure the network to meet the demands of the user and control costs. networkMaryland aims to provide the same service with lower costs than charged by outside providers. This is most beneficial for both Internet services and the InterLATA data circuits most agencies use to connect statewide offices. In addition to the higher bandwidth circuits and lower pricing, networkMaryland will provide other value added services in Phase II and beyond.

The creation and use of networkMaryland will benefit the State of Maryland as a whole. This technology will provide education with the opportunity to reach greater resources and push them further into the community. Agencies with offices throughout the state may be able to lower costs and focus that money elsewhere. The access to the Internet will open doors to new services such as the ability to host World Wide Web sites and the extensive information found on the Web. The future of Wide Area Network (WAN) in Maryland is networkMaryland.

3 - networkMaryland Overview

networkMaryland is a statewide high-speed backbone available throughout the State of Maryland to connect Public Sector customers' networks. The Public Sector is defined as State, county and municipal government agencies and departments, public libraries, public hospitals, public K-12 education, and higher education.

networkMaryland offers InterLATA transport and Internet services to the Public Sector.

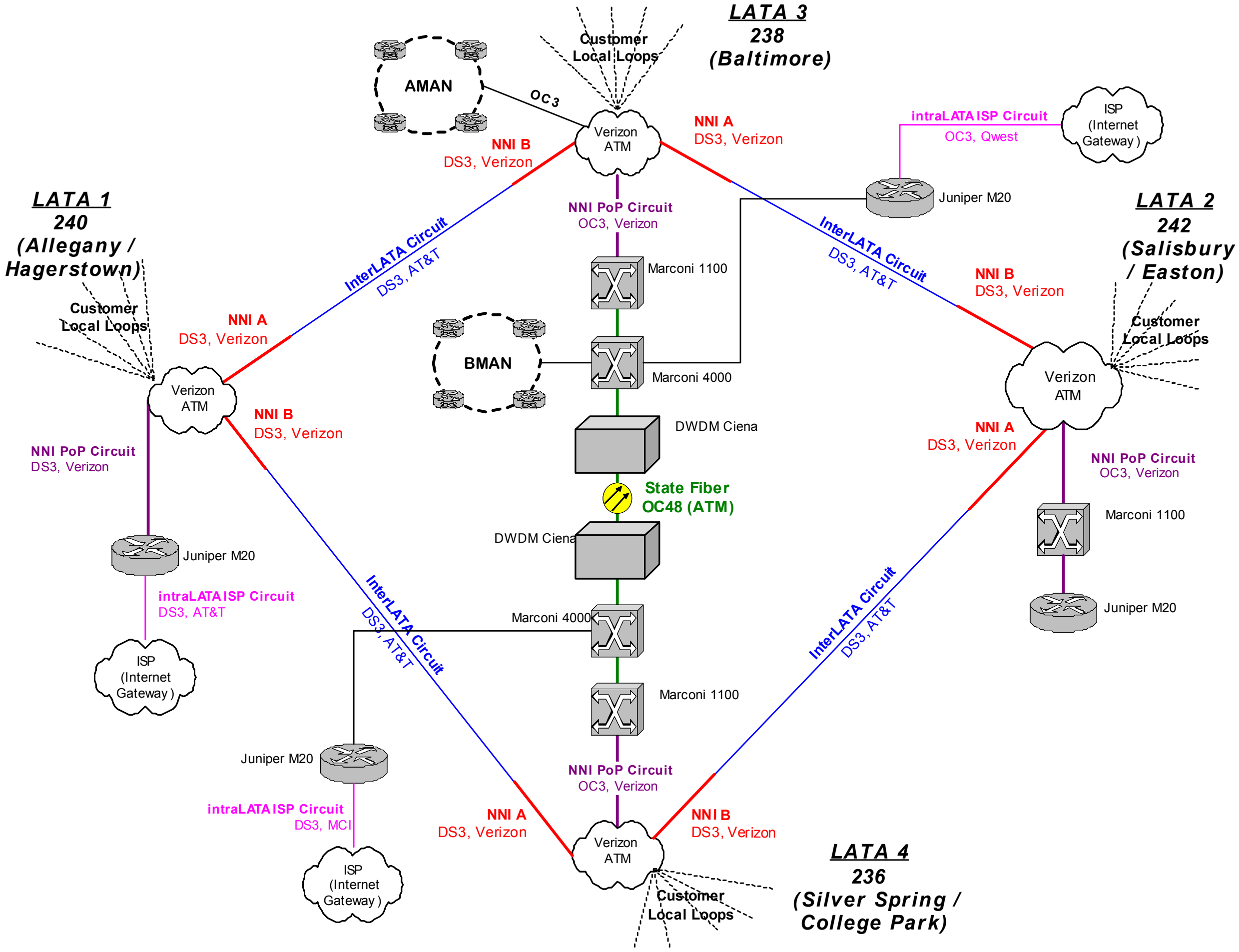

Figure 2. networkMaryland Design Overview

3.1 InterLATA Transport Services

networkMaryland is located in all 4 Local Access Transport Areas (LATAs). A LATA is a continuous geographic calling area established by a Federal Court with the divestiture of AT&T.

networkMaryland's InterLATA transport service is analogous to the services provided by a long distance phone carrier. The InterLATA transport service is designed to facilitate private WAN networks across a common infrastructure. networkMaryland serves only to provide a transport medium over which its customers can engineer their required network services. It is the customer's responsibility to design and manage the end-to-end network layer and route distribution protocols used to transport data across these services. networkMaryland supports ATM services across its infrastructure.

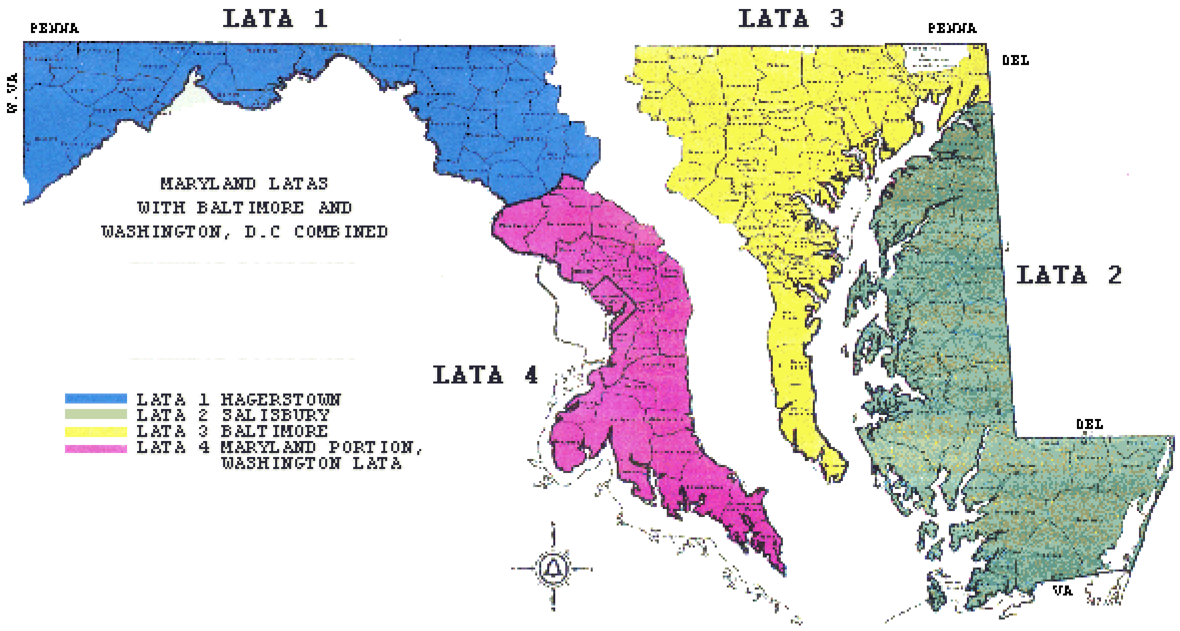

Figure 3. Maryland LATA Map

3.2 Internet Services

networkMaryland provides communication between the Internet and its Internet Service customers. networkMaryland's Internet Service is analogous to the routed services provided by a traditional Internet Service Provider (ISP). networkMaryland will provide the routed infrastructure over which its Internet Service customers will communicate to the World Wide Web community.

The routed Internet service is benign and security responsibility rests solely with the customer. networkMaryland serves only to facilitate connectivity and makes no attempt to govern what traffic is allowed or disallowed. It is the sole responsibility of the customer to govern access to and from their internal networks through the use of firewall rules.

3.3 Circuit Sizes

networkMaryland provides a variety of circuit bandwidths to allow for the flexible provisioning of circuits and proper utilization of resources. The ATM platform allows networkMaryland to provide circuits in the following bandwidths for InterLATA Transport and Internet Services:

- T-1: 1.5 Mbps

- 3-10 Mbps provisioned at 1 Mbps increments
- 45 Mbps provisioned at 5 Mbps increments

Circuits greater than 45 Mbps can be provisioned for customers collocated with networkMaryland, but this requires a Nonstandard Connection Proposal for approval (see section 4.1.4).

Circuit sizes can be determined by current usage and growth for the immediate future. Increases can be made in the future at the predetermined increments, based on the initial provisioning (Example: Purchase 2 Mbps of Internet, can be increased to 5 Mbps with a short service downtime for provisioning). The flexibility allows customers to reduce costs while maintaining the option for future growth.

4 - networkMaryland Connections

This section discusses the detailed interface requirements for each of the services provided by networkMaryland. The descriptions have been broken into physical and logical interface requirements.

4.1 Physical Connections

networkMaryland offers three methods of physical connectivity into a networkMaryland Point of Presence (POP) or a Metropolitan Area Network (MAN):

- Local Loop circuits provided by a public Local Exchange Carrier (LEC)
- Private fiber optic cable for direct connectivity
- Twisted pair copper (CAT 5) cable for collocation connectivity

Both the Baltimore MAN and the Annapolis MAN are collocated with networkMaryland. Section 4.1.4 discusses support for nonstandard connections to networkMaryland.

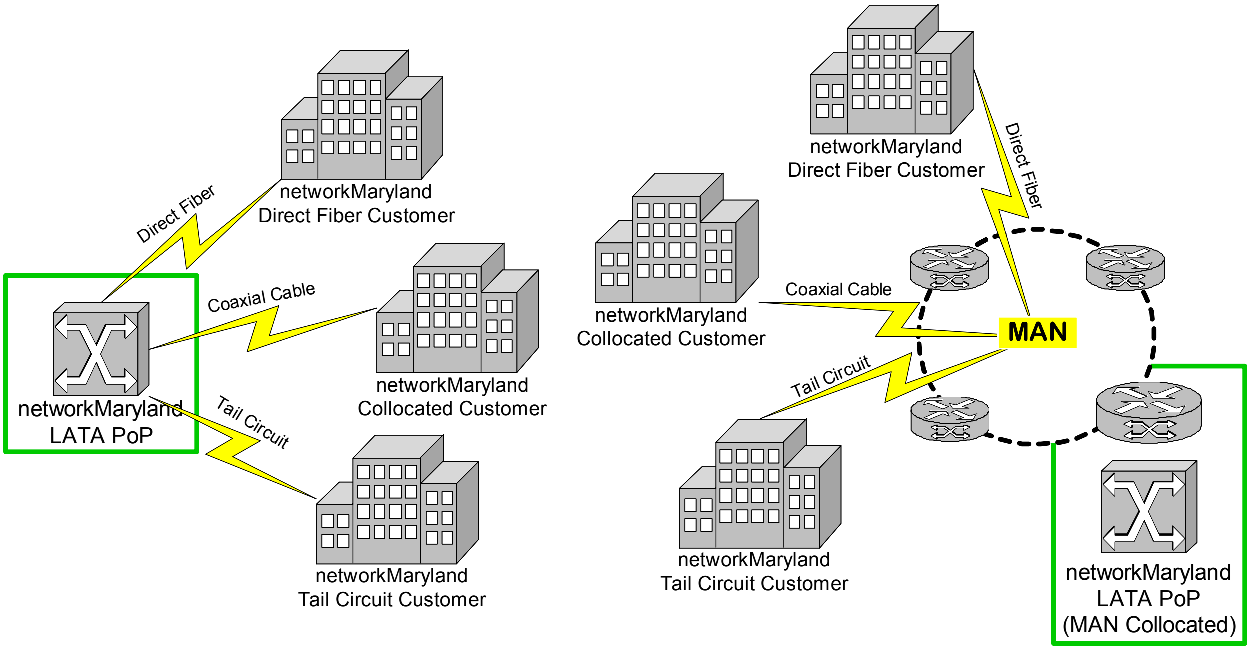

Figure 4. networkMaryland Connectivity Diagram

4.1.1 Local Loops

Customers of networkMaryland may contract with the LEC for native ATM services to connect to the nearest networkMaryland POP or MAN. State Agencies will order their local loop circuits through Department of Budget and Management Telecommunications. Non-State Agencies (other entities) wishing to connect to networkMaryland will order their own local loop circuit using the circuit ordering guidelines in the "Getting Connected Package". The "Getting Connected Package will be available for download from the networkMaryland web site (www.techmd.state.md.us/Technology/networkmdpage.htm). Interfaces to the LEC are governed by the specific requirements of that carrier. Currently, native ATM services are supported on DS1, DS3, or Optical Carrier interfaces (OC3 typically).

4.1.2 Direct Private Fiber

networkMaryland will support connections via direct fiber optic cable into any networkMaryland fiber PoP (currently Baltimore and College Park) and into the BMAN and AMAN. networkMaryland will provide support for both singlemode and multimode physical fiber optic interfaces. The standard line protocol to networkMaryland over direct fiber will be ATM. networkMaryland supports OC3c, OC12c, or OC48c. OC48c availability is limited to networkMaryland core PoPs.

4.1.3 Twisted Pair Copper Cable (CAT 5) for MAN Collocation

networkMaryland will support connections via the Baltimore and Annapolis Metropolitan Area Networks (MAN). The customer access within the Baltimore and Annapolis MANs are IEEE 802.3u and 802.3 compliant RJ-45 10/100 Ethernet interfaces. It is the customer's responsibility to extend (if required) the provided copper-based Ethernet interface(s). The Ethernet interfaces provided by networkMaryland support 802.1q VLAN trunking protocols as well as the Cisco ISL proprietary VLAN trunking protocol. The IEEE 802.1d spanning tree standard is utilized to ensure single path bridged network integrity.

Maximum Cabling Distance:

- 10BaseT Ethernet: Category 3 through Category 5 UTP: 328 ft (100m), 100-ohm STP: 328 ft (100m) half or full-duplex
- 10/100BaseTX and 100BaseTX Fast Ethernet: Category 5 UTP: 328 ft (100m), 100-ohm STP: 328 ft (100m) half- or full-duplex

4.1.4 Nonstandard Connections

networkMaryland can be engineered to support several other types of connections. Any non-standard connection will be handled on a case-by-case basis and be required to submit a proposal using the standard format (to be available for download on networkMaryland's public web site: networkMaryland Web Site: www.techmd.state.md.us/Technology/networkmdpage.htm) to networkMaryland's Advisory Group for review. DBM has the responsibility to make the final determination as to whether or not a request for a nonstandard connection will be granted.

The definition of a nonstandard connection is any proposal impacting networkMaryland assets that is not a customer request for service. One example is a resource-sharing proposal requesting or offering dark fiber "owned" by networkMaryland. Another example is a proposal from a state or local public entity requesting use of a networkMaryland-owned asset.

4.2 Routing and Addressing Guidelines

The following sections describe the network layer addressing and routing guidelines for each of the services offered by the networkMaryland system.

4.2.1 InterLATA Transport Services

With the circuit switched services network, the system does not participate in any network or higher layer protocols and therefore networkMaryland does not specify requirements on these protocols. It is the customer's sole responsibility to design and maintain the network layer environment that utilizes the networkMaryland Circuit Switched services.

4.2.2 Internet Services

Each customer of networkMaryland is assigned a block of IP addresses based on their requirements. networkMaryland provides the IP address and subnet mask assigned to the egress interface of the customer's termination equipment (the interface that connects to networkMaryland Internet POP—see Figure 4). The customer will be responsible for ensuring that all communications destined for the Internet are routed to the networkMaryland POP. networkMaryland provides the customer the necessary next hop IP address. networkMaryland will not enter into any dynamic IP routing relationship with any of its Internet customers. All routing information exchanged between a customer and networkMaryland is facilitated via the use of static routes.

The customer must ensure that the egress interface on their equipment be able to return both ICMP echo request (ping) responses as well as ICMP TTL expired messages (used in trace route) when the source address is a networkMaryland host. This will facilitate troubleshooting of customer connections.

5 - networkMaryland Demarcation

Customers must provide a minimum of one and up to three support points of contact. These support points of contact shall be used to notify the customer of problems, and shall be the persons through which the help desk is notified of problems.

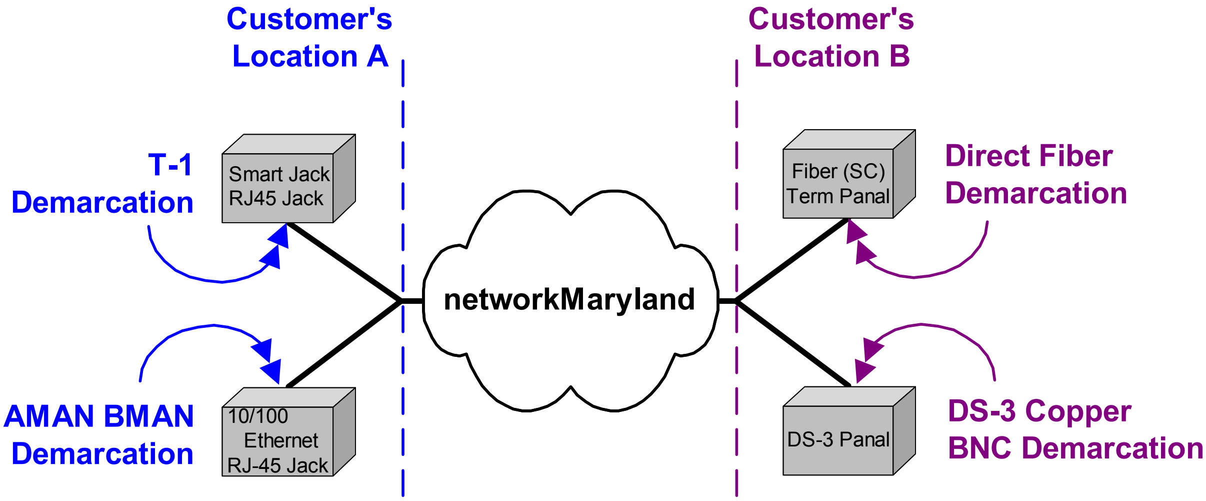

Figure 5. networkMaryland Demarcation Diagram

5.1 Local Loop Circuits

networkMaryland is responsible for ensuring communication up to and including the demarcation point established by the LEC. The customer is responsible for supplying, as well as maintaining and configuring, any equipment necessary to terminate the connection. This includes but may not be limited to the CSU/DSU, router, and circuit extensions to the customer's POP.

In the event a circuit problem is detected, the customer will contact the networkMaryland help desk . The help desk will identify the problem and take the necessary actions to restore the circuit. If a technician needs to be dispatched, customers will be required to provide access to the area in their facility that houses the demarcation equipment. Any such dispatching will be scheduled with the customer. If the problem is traced to customer-owned equipment (i.e. CSU/DSU, router, etc.) the customer will be contacted and informed of the findings.

In the event a routing problem is detected the customer will contact the networkMaryland help desk. The help desk will identify the problem and take the necessary actions to resolve the problem. networkMaryland is responsible for the routing and advertising of the customer's Internet subnets. The customer may be asked to provide configuration parameters for equipment relevant to the connection. Routing problems internal to a customer network are the responsibility of that customer.

5.2 Direct Private Fiber

networkMaryland is responsible for ensuring communication up to and including the demarcation point for users connecting via private fiber. The demarcation is typically a fiber distribution panel or, in the case of some customer co-location scenarios, an optical interface on the networkMaryland POP equipment. The customer is responsible for supplying, as well as maintaining and configuring, any equipment necessary to terminate the connection. This includes but may not be limited to the router, Ethernet switch, or ATM switch, as well as the fiber extensions to the customer's POP.

In the event a switching circuit problem is detected, the customer will contact the networkMaryland help desk. The help desk will identify the problem and take the necessary actions to restore the circuit. If a technician needs to be dispatched, customers will be required to provide access to the area in their facility that houses the demarcation equipment. Any such dispatching will be scheduled with the customer. If the problem is traced to customer-owned equipment (i.e. router, switch, etc.) the customer will be contacted and informed of the findings.

In the event a routing problem is detected (Maryland Government Intranet and Internet Services), the customer will contact the networkMaryland help desk. The help desk will identify the problem and take the necessary actions to resolve the problem. networkMaryland is responsible for the routing and advertising of the customer's Internet subnets. If necessary, the customer will be asked to provide configuration parameters for equipment relevant to the connection. Routing problems internal to a customer network are the responsibility of that customer.

5.3 Twisted Pair Copper (CAT 5) for MAN Collocation

networkMaryland is responsible for ensuring communication up to and including the demarcation point for users connecting via the Baltimore and Annapolis MANs. The demarcation point in the MANs is the RJ-45 10/100 Ethernet port located on the networkMaryland POP equipment. The customer is responsible for supplying, as well as maintaining and configuring, any equipment necessary to terminate the connection. This includes but may not be limited to the router or Ethernet switch as well as the CAT 5 twisted pair extension to the customer's POP.

In the event a switching circuit problem is detected, the customer will contact the networkMaryland help desk. The help desk will identify the problem and take the necessary actions to restore the circuit. If a technician needs to be dispatched, customers will be required to provide access to the area in their facility that houses the demarcation equipment. Any such dispatching will be scheduled with the customer. If the problem is traced to customer-owned equipment (i.e. router, switch, etc.) the customer will be contacted and informed of the findings.

In the event a routing problem is detected (Maryland Government Intranet and Internet Services), the customer will contact the networkMaryland help desk. The help desk will identify the problem and take the necessary actions to resolve the problem. networkMaryland is responsible for the routing and advertising of the customer's Internet subnets. If necessary, the customer will be asked to provide configuration parameters for equipment relevant to the connection. Routing problems internal to a customer network are the responsibility of that customer.

6 - networkMaryland Service Levels

The networkMaryland backbone is critical in supporting the business needs of state and local public entities by providing high-speed interLATA connectivity and intraLATA ISP access. This SLA establishes the obligations of networkMaryland to meet high standards of performance and outlines the responsibilities of using organizations. Additionally it describes the remedies available to users when the networkMaryland fails to deliver within prescribed parameters.

Definitions

- Network Operating Center (NOC) – the physical space, from which a large telecommunications network is managed, monitored and supervised. The NOC coordinates network troubles, provides problem management, and manages network changes.
- Permanent Virtual Circuit (PVC) – A logical connection from one port of the ATM network to another port of the ATM network
- Total Ingress Kilobytes – The total number of kilobytes (1000 bytes) offered by the ATM network
- Total Egress Kilobytes – the total number of kilobytes delivered by the ATM network across all PVCs
- Committed Burst Size (Bc) – The maximum amount of data (in bits) that the network commits to transfer under normal conditions
- Excess Burst Size (Be) – The maximum amount of uncommitted data (in bits) in excess of Bc that the network attempts to transfer under normal conditions
- Peak Cell Rate (PCR) – rate above which ATM cells are discarded
- Bc + Be Exceeded Kilo frames – Discarded frames due to excess data being sent above the maximum rate parameters of a given PVC
- Data Delivery Ratio or Rate (DDR) – The adjusted ratio of the total user data frames delivered across the frame relay network to the total user data frames offered to the frame relay network
- Cell Loss Ratio (CLR) – The ratio of cells unsuccessfully delivered across the ATM network to the total cells offered to the ATM network

Customer Requirements

Customers must provide a minimum of one and up to three support points of contact. These support points of contact shall be used to notify the customer of problems, and shall be the persons through which the help desk is notified of problems.

networkMaryland requires customers to provide access to network equipment as needed to perform routine and emergency maintenance and problem resolution. A contact list for agency internal personnel responsible for network operations is also required to ensure proper notification and access to network elements. We request that at least one member of each agency provide 24x7x365 access to the site. Those members of an agency not wishing to be notified of network problems 24x7x365 should specify so on the contact list. The contact list will be utilized by the NOC and DBM personnel to notify the customer of outages and network maintenance.

Maintenance Window

networkMaryland reserves the right to perform network maintenance that may be traffic affecting between the hours of 11 PM- 5 AM Sunday through Saturday. No maintenance will be performed without 5 business days' notice, unless an emergency situation requires such maintenance.

Service level Definition: Per-Circuit (PVC) Availability

For the ATM services provided to the user under a signed agreement, networkMaryland is committed to maintaining a per-PVC Availability of 99.5%. The availability applies to PVCs established between ATM endpoints on the managed network.

Measurement and Calculation

Per-Circuit (PVC) Availability is calculated as the percentage of time that PVC is capable of accepting and delivering information to the total time in a measurement period.

The calculation for availability for each of the PVCs in the user's network in a given month is as follows:

$$\frac{\textbf{(Hours in a Day x Days in a Month) – (Network Outage Time for a Particular PVC)}}{\textbf{(Hours in a Day x Days in a Month)}}$$

Network outage time is measured in wall clock time. Measured time starts when networkMaryland monitoring personnel or the using organization opens a trouble ticket, and ends at the time connectivity is restored. The help desk will enter trouble tickets within five (5) minutes of notification or NOC detection of a network outage.

Components Excluded

The following are excluded from any network outage time when calculating the Circuit Availability:

- The failure of any components beyond the CSU/DSU and/or monitoring device at the user's premises
- Network downtime during the Service Provider's scheduled maintenance windows
- The failure of any components which cannot be corrected due to inaccessibility to the customer site or customer equipment and other causes beyond reasonable control of networkMaryland
- Local Loop Circuits which another vendor such as Verizon, AT&T and WorldCom provides.
- Force Majeure (Natural Disaster, Acts of War or Terrorism and other forces beyond networkMaryland control).

Per PVC Availability Remedies:

Upon verification that a PVC is operating below the Committed Per-PVC Availability rate of 99.5%, networkMaryland shall evaluate the network and take corrective action to remedy the problem. NetworkMaryland shall have 5 Business days from the date of such verification to restore the Per-PVC Availability to the Committed Per-Circuit Availability.

Service Level Definition For: PVC Throughput

For ATM PVCs provided to the user under a signed agreement, networkMaryland is committed to maintain a Throughput of 100% (Committed Throughput).

Measurement and Calculation:

Throughput is measured in Kilobytes, where 1 Kilobyte is equal to 1000 bytes. The calculation for PVC Throughput is as follows:

$$\frac{\textbf{Egress Kilobyte Count x 100 percent}}{\textbf{Ingress Kilobyte Count – (Kilobytes above PCR or above Bc + Be)}}$$

The following are excluded from any determination of Throughput:

- Information lost due to failure of any components beyond the CSU/DSUs and/or monitoring device at the user's premises
- Information lost due to downtime during networkMaryland's scheduled maintenance windows
- The failure of any components which cannot be corrected due to inaccessibility to the customer site or customer equipment and other causes beyond reasonable control of networkMaryland
- Any PVCs or access channels added or reconfigured during the month
- Backup PVCs
- Force Majeure

PVC Throughput Remedies:

Upon verification that a PVC is operating below the committed Per-PVC Throughput rate of 100%, networkMaryland shall evaluate the network and take corrective action to remedy the problem. NetworkMaryland shall have 5 Business days from the date of such verification to restore the Per-PVC Throughput to the committed Per-Site Throughput specification.
Service Level Definition For: Mean Time To Respond in the event that on-site response is necessary, networkMaryland will maintain a maximum response time of 2 hrs, 3 hrs and 4 hrs for Region A, Region B, and Region C locations, respectively.

- **Region A Counties:** Anne Arundel, Baltimore, Prince Georges, Howard, Calvert, Montgomery, and Queen Anne's
- **Region B Counties:** Carroll, Charles, St. Mary's, Harford, Fredrick, Washington, Talbot, Caroline, Kent, and Dorchester
- **Region C Counties:** Allegany, Garrett, Cecil, Wicomico, Somerset, Worchester

Elapsed time is measured from the time a particular trouble ticket is opened to the time assistance arrives at the problem site. The Mean Time to Respond calculation is as follows:

$$\frac{\textbf{Total Time (in Hrs) to Respond for All Trouble Tickets That Require On-Site Maintenance}}{\textbf{Total Number of Trouble Tickets That Require On-Site Maintenance}}$$

Upon verification by networkMaryland that the response level is below the specification, corrective action shall be taken to remedy the problem. NetworkMaryland shall have 5 business days from the date of noncompliance to correct the deficiency.

Service Level Definition For: Mean Time to Repair

NetworkMaryland will maintain a maximum of 4 hrs repair time for service problems that do not require on-site dispatches and a maximum of 8 hrs repair time for service problems that require on-site dispatches. In the event of a fiber optic cut, 12 hrs may be required to restore service.

Elapsed time is measured from the time the trouble ticket is opened to the time service is restored to normal performance. The calculation for Mean Time to Repair is as follows:

Mean Time to Restore (Without On-Site Dispatches) =

$$\frac{\textbf{Total Outage Time (in Hrs) for All Trouble Tickets That did not Need On-site Dispatches}}{\textbf{Total Number of trouble Tickets that did not Need On-Site Dispatches}}$$

Mean Time to Restore (With On-Site Dispatches) =

$$\frac{\textbf{Total Outage Time (in Hours) for All Trouble Tickets That Needed On-Site Dispatches}}{\textbf{Total Number of trouble Tickets That Needed On-Site Dispatches}}$$

Excluded Items:

- Test and inquiry trouble tickets
- “No trouble found” trouble tickets

Upon verification by networkMaryland that the actual Mean Time to Repair level is below the specification, networkMaryland will take corrective action. NetworkMaryland shall have 5 business days from the date of noncompliance to report the cause of deficiency and take corrective action.

7 - networkMaryland Acceptable Use Policy (10/2/02)

These statements represent the acceptable use policy of networkMaryland. All organizations connected to networkMaryland must comply with this policy. Each organization is responsible for the activity of its users and for ensuring its users are aware of this policy. Reference to and acceptance of this policy must be stated in the acceptable use policies of all agencies connecting to networkMaryland. Any determination of inappropriate use or violations of this policy shall be promptly reported to the Department of Budget Management for appropriate action up to and including termination of service.

- Use by Members must be consistent with the purposes and mission of networkMaryland cannot put the above in there until response from legal counsel.
- Members may not transmit any material that:
    - Violates any applicable local, state, national or international law or contract and license agreements.
    - Threatens or encourages bodily harm or destruction of property.
    - Promotes a business, products or services not consistent with networkMaryland's service mission.
    - Constitutes copyright or trademark infringement or other proprietary rights of any third party.
- Members may not resell services.
- Members may not engage in any unauthorized or unplanned network disruptions or activities that interfere with the ability of other users to make effective use of the network.
- Commercial for profit activity of any kind is forbidden. At cost or cost recovery services require the review of the networkMaryland Advisory Group and approval of the Department of Budget Management.
- Repeated, unsolicited and/or unwanted communication of an intrusive nature, including spamming, is not acceptable.
- Members will file incident reports related to any local network outages or disruptions.
- Members have read and are in compliance with the technical requirements, including IP addressing, for connecting to networkMaryland.
- Members may not reveal documents or information gained as a connecting agency that may show network vulnerability.

In an emergency and in order to prevent further possible inappropriate, unlawful or damaging network activity, networkMaryland may temporarily disconnect a Member agency. If this is deemed necessary by networkMaryland staff, every effort will be made to inform the Member prior to disconnection, and every effort will be made to re-establish the connection as soon as it is mutually deemed safe.

NetworkMaryland reserves the right to revise, amend, interpret or modify this AUP and other related policies. Members will be notified of any AUP changes through letter. The Department of Budget Management is the final authority on questions of acceptable use of the network. Periodic audits may be conducted by the Department of Budget Management to enforce this policy.

8 - Customer Responsibilities

Customer Premise Equipment:

The networkMaryland infrastructure provides a variety of ways for a customer to connect to the network for interLATA transport and Internet Services. The structure of the network requires customers to provide their own Customer Premise Equipment (CPE) that is compatible with networkMaryland interfaces and/or Local Loop provider. The CPE is to be available on the scheduled turn-up date to ensure end-to-end testing is possible. The configuration of CPE equipment will be the responsibility of the customer prior to the scheduled turn-up date. This may require scheduling contractors or inside personnel to meet this requirement.

Ordering of Circuits:

Customers connect to networkMaryland using the guidelines outlined in the Getting Connected Package, available for download on the networkMaryland public web site (www.techmd.state.md.us/Technology/networkmdpage.htm).

Security:

Individual PVC circuits provide information security across networkMaryland's infrastructure. The PVC circuit is an open pipe that allows data to pass from end-to-end as presented at the termination ports. The customer must provide any additional security to protect the integrity of the data. Each type of circuit provided by networkMaryland has different security needs.

- InterLATA Transport: This solution is secure by the nature of the ATM infrastructure. Any information that is sensitive in nature may require additional security provided by encryption or other hardware/software products.
- Internet Services: The connection to the Internet requires special precautions to eliminate any security risks. The customer must provide a firewall or other hardware/software solution to protect against network intrusion. NetworkMaryland is not responsible for any acts against a customers network.

Customer Network Management:

The management of the customer network is the sole responsibility of the customer. networkMaryland manages the network up to the demarcation point or local loop circuit termination. The customer controls customer network equipment, including the CPE connecting to networkMaryland. Any failures of this equipment or required upgrades will be the responsibility of the customer.

Facility Access:

The customer of networkMaryland is responsible for providing access to the demarcation points or circuit termination points for vendors, networkMaryland contractors and employees. Any after-hours access will be schedule with the customer prior to the access time with sufficient notice. This access will allow for installation, testing, and circuit repair and site surveys.

9 - State of Maryland Data Security Policy (8/16/99)

STATE POLICY: INFORMATION PROCESSING RESOURCES SECURITY

I. Authority

A. **Governor's Executive Order 01.01.1983.18, which created the State Data Security Committee to establish State data security standards.**

B. **State agency information system security practices as enumerated by the State Data Security Committee.**

C. **Article 27, Sections 45A and 146 of the Annotated Code of Maryland.**

II. Objective

A. **The purpose of the Policy is:**

1. To assign responsibility, on an agency/institution-wide basis, for implementing the procedures required by the State Policy issued by the State Data Security Committee.
2. To protect the integrity of the State agency and institution computerized record systems.

B. **This policy is applicable to all units of the Executive Branch of State Government.**

III. Policy Statement

In recognition of the fact that information is valuable resource in the efficient operation of State government at all levels, and the fact that the privacy of individuals is directly influenced by the collection and use of personal records, it is the policy of the state of Maryland to protect sensitive data from unwarranted disclosure and to protect information processing resources from abuse or damage by natural of other causes.

The following procedures shall be adhered to by all agencies within the Execute Branch of Maryland State Government.

IV. Procedure

Each agency administrator, head of a commission and the other directing authority of State Government 1) shall be responsible to formulate directives to properly protect information processing resources in accordance with the State Computerized Record System Security Requirements and the requirements and recommendations contained therein, and 2) appoint a Security Officer as required buy the Governor's Executive Order.

V. State Agency Data Systems Security Practices

A. Agency Computer Software and Records Security

THE FOLLOWING SECURITY PRACTICES ARE REQUIRED for all computer systems including mainframes, minicomputers, data communications facilities, local area networks (LANs) file servers, microcomputer network nodes, and standalone microcomputers (desktops or notebooks/portables) which contain critical or sensitive data files. (Management must identify what are critical or sensitive data files.)

1. Written procedures to safeguard application system data files must be prepared and followed.

2. The documentation for each application system must address sufficient controls for maintaining the security of source documents, before, during, and after the data entry process, and the distribution of all output.

3. All source and object programs must be maintained in a manner that prevents unauthorized access.

4. Each agency is required to maintain a list of its data processing applications and files.

5. Each agency is required to store copies of agency computer files and programs on a routine basis at an off-site location. An off-site location must be in a building other than the one that houses the primary computer files and programs.

6. Each agency is required to store at an off-site location copies of data systems documentation, which would be vital in continuing the operation of the systems in an emergency situation, which has resulted in the destruction of the original documentation.

7. When capabilities are available, each agency must use an automation method)e.g., a security software package) to safeguard application system data files.

THE FOLLOWING SECURITY PRACTICES ARE REQUIRED in all instances where agencies have standalone microcomputers (desktops or notebooks/portables) or LAN file servers and microcomputer network nodes.

8. Because notebook/portable microcomputers are highly susceptible to theft, the devices must b e protected via the use of access-control software, passwords and a boot or power-on password where feasible and practical. A power-on or boot password protects the device from use of a DOS or system bootable diskette to bypass the computer's access control software.

8b. The storage of network modem telephone numbers and network passwords in unsecured standalone microcomputers (desktops or notebook/portables) is strictly forbidden.

9. All agency software and files on removable media must be put into a locking storage unit when not in use or be maintained in areas that are locked when not in use.

10. To minimize the chance of computer viruses being introduced into microcomputers only authorized and properly licensed personal computer software packages are to be used on PC's. Authorized PC software packages are those developed and approved by agency management or those obtained from reliable and responsible vendors, e.g. State software B OA vendors, nation-wide distributors, etc. that are committed to assuring product quality. The use unauthorized or unlicensed PC software and programs (i.e., software obtained from computer bulletin boards, friends, other employees, etc.) is strictly forbidden. Only work related PC software approved by agency management is to be installed on State microcomputer equipment.

11. As a means of recovering from a computer virus attack or disaster, backup procedures must be implemented on a routine basis for agency software and files stored in PCs and LANs.

12. All users of microcomputers must use a virus scan/protection program on a regular basis to minimize damage caused by virus attacks and to scan data files for viruses entering the computer. All virus scan/protection programs used for this process must be updated on a regular frequency. The frequency of the updates is a minimum of every two years.

13. All employees utilizing personal computers must sign the State of Maryland Software Code of Ethics Form (part of the Department of Budget and Management's Policy Number 95-1), which states that unauthorized duplication of copyrighted computer software violates the law and is contrary to the State's standard of conduct.

14. When a sensitive or critical PC application is created, the application author is responsible for documenting the application. Documentation may differ slightly from one type of application to another; however, all documentation must contain the following elements:

- A written description of the application
- Step by step instructions on how to use the application
- The names and location of the PC files
- A copy of the output
- The backup procedure for the application

The following documentation is suggested:

- A log of revisions (the log should include the name of the application, the original author, the date it was created, the date of each revision, the name of the individual who revised the application, and the reason for the revision).

15. A written plan to assure that all its critical and sensitive application is "Year 2000" compliant must be adopted by each agency by December 31, 1997. Security software supporting those critical and sensitive applications must be "Year 2000" compliant.

16. A written PC security policy must be promulgated and adopted by each agency. This policy must include, as a minimum, items A.8 through A.15 above.

THE FOLLOWING SECURITY PRACTICES ARE RECOMMENDED.

Security should be considered in the design and development of each computerized record system. All agency programs should be maintained in a library, which provides an audit trail of changes made to the programs. Whenever appropriate, each document which is used for initiating error corrections to computer records should contain a statement of justification and proper authorizations.

Agencies are encouraged to tie standalone PC's together into a Local Area Network (LAN) so that software can be loaded and managed centrally, critical and sensitive files can be stored and backed up more easily and sensitive files and applications can be more readily protected from virus attached and other security threats.

B. Agency Computer Hardware Security

THE FOLLOWING SECURIRY PRACTICES ARE REQUIRED in all instances where agencies have standalone or network microcomputers, notebook/portable microcomputers and computer terminals located in areas other than within secured computer facilities.

1. Agencies must take appropriate preventative actions to guard against damage to, or theft of, these devices.
2. Because notebook/portable microcomputers are highly susceptible to theft, none of these devices are to be lift in unsecured areas while not in use e.g., the back seat of a parked vehicle.
3. Computer terminals, standalone microcomputers and microcomputer network nodes must not be left logged on to computer systems when unattended.
4. When capabilities are available, computer terminals and microcomputer network nodes must be automatically logged off by the operating system when there is no terminal activity for pre-designated period of time.
5. When disposing of microcomputer processing units, an agency must take the appropriate action to delete all of the data that is contained on the processing unit's hard drive.
6. In a telecommuting environment, an agency must provide the same level of security on the microcomputer used at home as the microcomputer used in the workplace.

C. Password, Sign-on and Access Security

THE FOLLOWING SECURITY PRACTICES ARE REQUIRED for State agencies, which utilize remote connectivity and data communications capabilities.

1. Individual user passwords must be used for every session, transmission or access to application systems.

THE FOLLOWING SECURITY PRACTICES ARE REQUIRED for State agencies where password, sign-on access control security features are installed.

2. Passwords must be changed periodically.
3. The assignment of passwords must be tightly controlled.
4. Users must be advised that all passwords must be kept confidential and secure. The procedure for assigning passwords must reflect that efforts are made to retain the confidentiality of passwords.
5. Terminal and microcomputer network node users of the computer facilities must be restricted to accessing only files that they are individually authorized to access and also be limited to authorized operations that they may perform on or with these files.
6. System administrators must maintain a formal, written audit trail of all security access control activities on the system. The audit trail shall include, but not be limited to maintaining a log of all changes to all user access rights/logonid's and requests to change user passwords as long as the user access rights/logonid's for at least two years or until audited by the Legislative Auditor and maintaining a log of all security exceptions/violations for at least two years or until audited by the Legislative Auditor.

7. Agency management of a designee of agency management must periodically review and document the security privileges, data file and programs access control rights of all personnel authorized to interface with critical or sensitive application systems, files and programs. Agency management personnel that perform this review task must not include persons who manage the access controls. The review documentation must be retained for at least two years or until audited by the Legislative Auditor.

THE FOLLOWING SECURITY PRACTICES ARE RECOMMENDED.

Password management software that allows system administrators to define the rules governing how users pick their passwords is available. Use of these systems strengthens data security significantly. With appropriate password management, administrators can specify that 1) passwords are not actual names or words, 2) are of a minimum and maximum length, 2) are not used over again, 4) contain at least one number, and 5) are not composed of repeating digits. Adequate password management also permits the development of special password validation programs for processing unique applications. It is therefore recommended, where capabilities exist, that administrators implement all or some of the aforementioned password management techniques to improve password security.

Also, it is important to ensure that users are who they say they are when they sign-on to a system. This includes incorporating the ability to check users authorization every time they access a new system resource. Software is available that are aimed at identifying possible intruders and preventing unauthorized entry into systems. Recommended features include 1) preventing a single user from signing on to more than one workstation at a time; 2) restricting individual users to workstations with specific addresses; and 3) scheduling capabilities that lets administrators specify the times of day when users are allowed to sign-on to a system. It is therefore recommended, where capabilities exist, that administrators use the aforementioned sign-on techniques to the maximum extent possible.

D. Agency Information Technology Personnel Practices

These required and recommended security practices apply to all employees (contractual and permanent) and information technology consultants who interface with application systems that have been identified by agency management as being critical or sensitive. The types of duties or functions of personnel addressed by the foregoing shall include, but not be limited to security officers who grant system access rights to others, programmer-analysts, systems programmers, database administrators, network mangers, information technology consultants and other personnel identified by agency management who have rights to access critical or sensitive application systems, files and programs.

THE FOLLOWING SECURITY PRACTICE IS REQUIRED.

All agency security officers must satisfactorily complete a course of instruction specified by the State Security Committee.

THE FOLLOWING SECURITY PRACTICES ARE RECOMMENDED

1. It is recommended that each agency have a designated Certified Software Manager. A Certified Software Manager is defined as an individual who has participated in the Certified Software Manager Course Certification Exam program offered by the Software Publisher’s Association (SPA) through its outsourcing provider, Fortress

Technologies, at an approximate cost of $400 per person. The one day, 6-hour course is designed for managers and specialists working in areas of MIS, microcomputing, computer services and technical support in addition to auditors, counsel, and others responsible for software compliance. The course defines the skills necessary to be a Certified Software Manager so an individual can gain the full benefits of software and avoid the legal penalties of mismanaging it. By successfully completing the course an attendee will:

- Understand copyright law and licensing agreements
- Understand the software audit process
- Understand the benefits and processes of software asset management
- Develop a workable software management plan

Once attendees have completed the course, they must pass a one-hour exam in order to be certified. Sylvan Prometric will administer the exam for an additional $100 fee that may be paid directly to Sylvan. The exam must be scheduled after the course is taken.

Course materials attendees will receive include the following:

- A 300-page comprehensive student guide
- SPA's anti-piracy video, posters, brochures and article reprints
- SPAudit software to accelerate the self-audit process saving staff time
- "A roadmap for Buying Software poster and guide

SPA offers the one day course during the year in Washington D.C. In order to receive a current schedule of course dates, agencies can contact the SPA at the following address: http://www.spa.org

2. If, in the opinion of agency management, a prospective employee will be interfacing with a sensitive or critical computer application, a criminal history record check should be conducted.

NOTE: A criminal history record checking service is offered, at a fee, to state agencies by the State of Maryland's Department of Public Safety and Correctional Services (DPSCS). The procedure for this service is entitled "Criminal History Record Checks For Prospective State Employees". Request forms that must be signed by the appointing authority of a state department of agency are available from:

Customer Service Unit
CJIS Central Repository
P.O. Box 5743
Pikesville, Maryland 21208-0195
Phone #: 410-318.6021

State agencies are encouraged to hire applicants on a conditional basis pending receipt of the satisfactory criminal history record check.

Background checking should be performed for final candidates for these positions prior to selection for employment. Background checking is contacting previous employers, references, and other appropriate individuals or organizations to verify the education, training and/or experience needed to meet minimum qualifications.

Agency personnel with access to critical or sensitive data files should be advised periodically as to how data security violations should be reported. Whenever feasible, employees that work with security sensitive computerized record systems should be periodically rotated in their job functions. Agency data systems security procedures, which pertain to agency personnel, should also apply to temporary and contractual personnel.

To provide appropriate degrees of internal control over data processing operations, agency management should segregate functions so that information technology personnel who perform systems maintenance functions are not performing user type functions as a regular part of their duties and responsibilities. In addition, agency management should separate the following data processing duties and responsibilities among several employees:

- Performing computer operations functions
- Maintaining application program software
- Maintaining operating systems and databases and
- Performing data processing security functions

VI. State Computer Facility Security Practices

This section applies to all State mainframe, minicomputer, data communications facilities and Local Area Network (LAN) installations that process critical or sensitive data files, (Management must identify what are critical or sensitive data files).

A. Physical Security of Computer of Data Communications Operations Area

THE FOLLOWING SECURITY PRACTICES ARE REQUIRED.

1. All fire safety devices must be approved and periodically checked by the State Fire Marshal.

2. The facility must have a written procedure for the disposal of its own data processing materials.

THE FOLLOWING SECURITY PRACTICES ARE REQUIRED only at computer facilities with separated, restricted computer or data communications operations areas.

3. The facility is required to control the access to the computer or data communications operations area, permitting entry of authorized personnel only. Entry of maintenance and custodial personnel must be controlled. Former employees and visitors to the computer operations or data communications area must always be escorted.

4. If a building with a separate facility has security guards, these guards are to be scheduled to make routine checks of the facility. Management must identify the level of routine checking to be performed by security guards (e.g., perimeter checking only, full physical access, visual inspection, etc.).

5. If security guards are not available, an access alarm is to be used when the facility is unattended.

THE FOLLOWING SECURITY PRACTICES ARE RECOMMENDED.

When the size or schedule of the computer or data communications facility does not permit all employees to be known and recognized, every employee should be required to display an official identification containing a photograph of the employee.

The computer or data communications operations area should contain smoke and/or heat sensors for early detection of a fire. An automatic fire-suppressing system should be installed. The space under any raised flooring should be inspected periodically for possible hazards.

Some types of network protocol analyzers and test equipment are capable of monitoring (and some, of altering) data passed over the network. Use of such equipment should be tightly controlled since they emulate terminals and can monitor and modify sensitive information, or contaminate data.

B. Contingency Planning

THE FOLLOWING SECURITY PRACTICES ARE REQUIRED.

1. The computer or data communications facility management must routinely assess the relative probability of significant hazardous events occurring at the facility. As a minimum, a significant hazard means fire, flood, unauthorized entry or access, power failure and man made (e.g. terrorist) or natural disasters.
2. The computer or data communications facility management must routinely assess the vulnerability of the facility to the specified significant hazards.
3. The computer or data communications facility management must have a contingency plan which addresses and prescribes actions to be taken for all significant events which management has determined could place the facility at risk. Specifically, the contingency plan must address personnel, hardware, software, data, remote connectivity, and data communications networks. The plan also must contain a section dealing with the recovery from a major disaster that would render the facility unusable and require restarting operations at an alternate site. The major disaster recovery section must address the initial response, restart procedure, personnel assignments, backup resources and facilities, and emergency vendor contracts/vendor agreements.
4. The computer or data communications facility management must periodically validate the contingency plan. The following guidelines, listed in priority order, are to be used in conducting the validation:
   - Actual, live, full scale disaster recovery test exercises must be used wherever feasible and practical or,
   - Partial recovery test exercises or simulations (e.g. tabletop exercises) of disaster recovery procedures must be used when it is impractical to conduct full-scale disaster recovery tests.

The computer or data communications facility management must periodically update the contingency plan to reflect deficiencies noted during validation tests and to assure that the plan is current, viable and complete.

THE FOLLOWING SECURITY PRACTICES ARE RECOMMENDED.

5. As an aid in securing upper management's support for on-going contingency planning efforts, the computer or data communications facility management should consider performing a risk analysis, which will assist in striking an economic balance between the impact of risks and the cost of protective measures. A well-executed risk analysis

will improve security awareness, identify assets, significant hazardous events and controls, improve the basis for decisions and justify expenditures for security. Risk analysis steps include the following:

- Identify critical information assets
- Determine significant hazardous events
- Estimate likelihood of occurrences of significant hazardous events
- Document the impact of a loss of critical information assets (compute annual loss expectancy)
- Identify applicable cost associated with controls to be implemented
- Project annual savings of controls

During the assessment of the contingency plan, the computer or data communications facility management should consider the merits of having arrangements for alternative computer processing capabilities at an off-site location for emergency needs. If this option is cost effective and practical, a formal agreement should be prepared with the organization responsible for the off-site facility.

Contingency planning in Client Server environments is more complicated than it is for a mainframe data center. Many Client Server systems utilize technologies produced by several vendors in a distributed computing environment, thus multiple points of failure may occur which can magnify the scope and severity of problems. An agency's Client Server disaster recovery plan is best managed by centralized information technology system groups.

To plan for unseen calamities, the computer or data communications facility management should determine where critical Client Server information is stored and how it is used. It is recommended that:

- Physically distributed servers be pulled back into a centralized, controlled environment wherever feasible or practical to better manage and protect information, improve security, data integrity and asset tracking.
- Software tools should be employed in Client Server environments to help create ways to protect information and systems. These software tools can help agencies choose what is most essential to recover.

The computer or data communications facility management should consider installing fault tolerant hardware and fault management software features in all critical and sensitive networks and application systems to guard against data loss and to provide for high systems availability.

Network and application system fault tolerant hardware features that agencies should consider installing include, but are not limited to, are:

- Error correction code (ECC) memories
- Redundant arrays of inexpensive disks (RAID) technologies
- Hot-pluggable and hot spare disks
- Dual redundant power supplies sized to support fully loaded configurations
- Smart uninterruptible power supplies

Network and application fault management software features that agencies should consider installing include, but are not limited to, the capability to monitor and report on the status of:

- Memory
- Processors
- Disk storage devices
- Power usage
- Network equipment
- Internal temperatures of processor units

C. Computer Records

THE FOLLOWING SECURITY PRACTICES ARE REQUIRED.

1. When capabilities are available, the computer system must provide an audit trail of all authorized and unauthorized attempted accesses to computer resources.
2. When capabilities are available, the computer system must use an automated method (e.g., a security software package) to safeguard computerized files.

D. Remote Connectivity and Data Communications

THE FOLLOWING SECURITY PRACTICES ARE REQUIRED for State computer facilities, which utilize remote connectivity and data communications.

1. The computer facility must provide procedures to control access from the remote user locations during hours that remote user locations are closed.
2. Each user access must be terminated if the security code is still incorrect after a specific number of user attempts to log on.
3. Before being prompted for the user name and password, a banner must appear warning users of system monitoring procedures and State laws that apply to breaches of computer security. For example:

WARNING: Unauthorized access to this computer is in violation of Article 27, Sections 45A and 146 of the Annotated Code of Maryland. This system is being monitored. Anyone using this system expressly consents to such monitoring. Detection of unlawful conduct may be referred to law enforcement officials.

THE FOLLOWING SECURITY PRACTICES ARE RECOMMENDED

User access logs should be regularly reviewed by an individual(s) outside of the computer operations area.

E. Dial-up Lines Access

THE FOLLOWING SECURITY PRACTICES ARE REQUIRED for computer facilities, which have dial-up communication lines.

1. The computer facility management must control the distribution of the computer telephone number used for a critical or sensitive application system. In these instances, the computer facility procedures for distribution the computer telephone number must reflect that efforts are mad to retain the confidentiality of the telephone number.
2. When capabilities are available or can be reasonably acquired, dial-up activity sessions must be terminated when the telephone is hung up or the carrier is dropped.

3. When capabilities are available or can be reasonably acquired, each dial-up connection must be broken whenever an unauthorized attempt is made to access a facility's computer.

4. Any system implemented for the purpose of providing electronic services for the citizens of the State via public dial-in access or through a connection to the Internet should be isolated/protected from an agency's internal computer network. This should be accomplished by ensuring the system has no internal network connection or is protected by a properly implemented networks or application level firewall that enforces a responsible access control policy.

THE FOLLOWING SECURITY PRACTICES ARE RECOMMENDED

5. Systems accessible from dial-up terminals are particularly vulnerable to unauthorized access since the call can be initiated from virtually any telephone instrument. Official users of dial-up facilities should be distinguishable from public user if they are to be given access rights greater than those given public users. For services other than those authorized for the public, users of dial-up terminals should be positively and uniquely identifiable and their identity authenticated to the system begin accessed. This should be implemented via a two level security procedure consisting of using either a call back facility or a Public Data Network (PDN) service to access the system. When using a call back facility, official users should be provided an automatic hang-up and call back feature, which calls back to only pre-authorized numbers. When using a PDN service, a separate, network User ID and user address code should be provided to official users by the PDN service. This is in addition to the computer system's User ID and password, which is provided and maintained by the computer facility.

6. An agency should exercise a great deal of care in deciding what information can be properly housed on a publicly accessible system. The agency's assistant attorney general should be involved in this decision making process.

10 - Next Steps

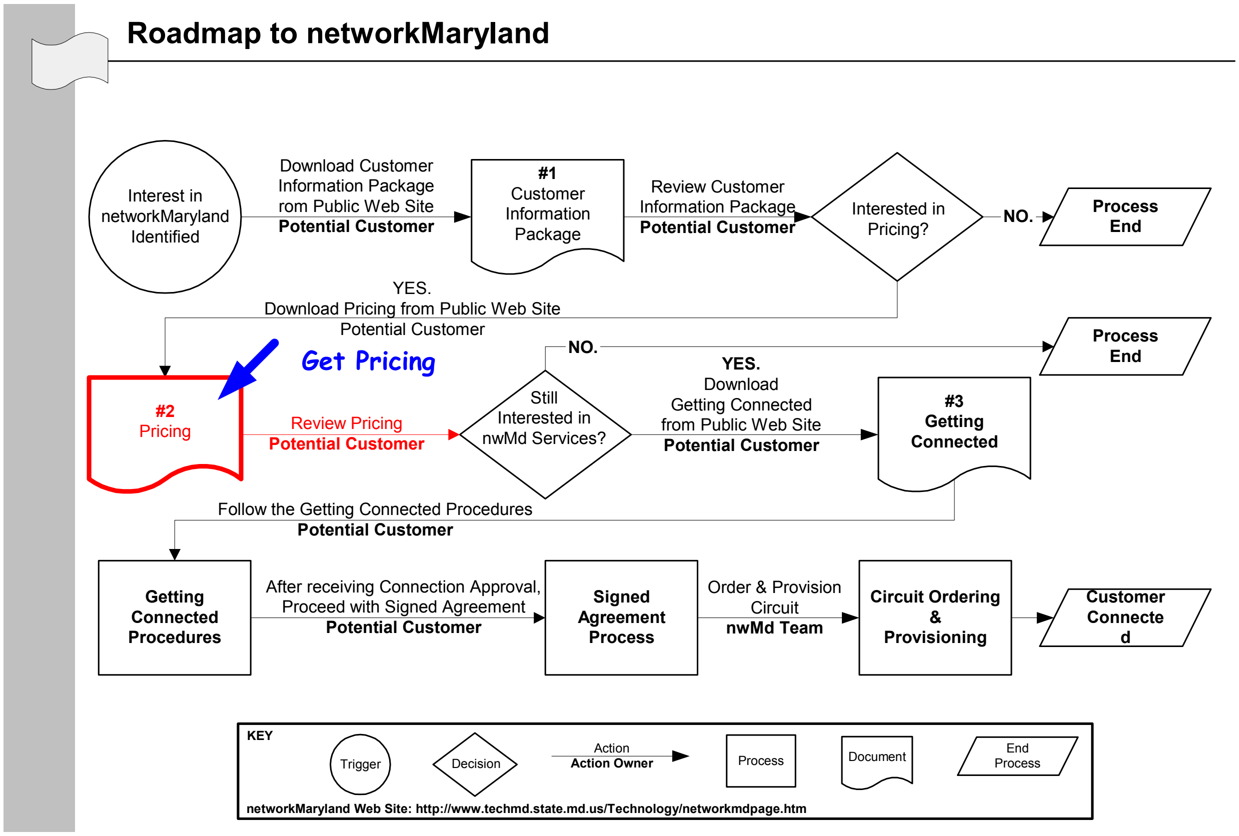
Roadmap to networkMaryland
Interest in networkMaryland Identified
Download Customer Information Package rom Public Web Site
Potential Customer
#1 Customer Information Package
Review Customer Information Package
Potential Customer
Interested in Pricing?
NO.
Process End
YES.
Download Pricing from Public Web Site
Potential Customer
Get Pricing
#2 Pricing
Review Pricing
Potential Customer
NO.
Process End
Still Interested in nwMd Services?
YES.
Download Getting Connected from Public Web Site
Potential Customer
#3 Getting Connected
Follow the Getting Connected Procedures
Potential Customer
Getting Connected Procedures
After receiving Connection Approval, Proceed with Signed Agreement
Potential Customer
Signed Agreement Process
Order & Provision Circuit
nwMd Team
Circuit Ordering & Provisioning
Customer Connecte d
KEY
Trigger
Decision
Action
Action Owner
Process
Document
End Process
networkMaryland Web Site: http://www.techmd.state.md.us/Technology/networkmdpage.htm

Figure 6. Roadmap – Get Pricing